INFORMATION AND PRIVACY COMMISIONER OF NUNAVUT

ANNUAL REPORT 2008/2009

Respectfully submitted by:

Elaine Keenan Bengts

Information and Privacy Commissioner of Nunavut

NUNAVUT INFORMATION AND PRIVACY COMMISSIONER

5018 - 47th Street
P.O. Box 262
Yellowknife, NT
X1A 2N2

May 25, 2009

Legislative Assembly of Nunavut
P.O. Bag 1200
Iqaluit, NU
X0A 0H0

Attention: The Honourable James Arreak
Speaker of the Legislative Assembly

Dear Sir:

I have the honour to submit my Annual Report as the Information and Privacy Commissioner of Nunavut to the Legislative Assembly for the period April 1, 2008 to March 31st, 2009.

Yours truly,

Elaine Keenan Bengts
Nunavut Information and Privacy Commissioner

INDEX

	Page
Commissioner's Message	1
The Role and Mandate of the Information and Privacy Commissioner	5
Access to Information	6
Protection of Privacy	8
Requests for Review	8
Making an Access to Information Request	10
Review Recommendations Made	11
Review Recommendation 08-43	11
Review Recommendation 08-44	12
Review Recommendation 08-45	13
Review Recommendation 08-46	14
Looking Ahead	16
Privacy Oversight	16
Time for Requesting Reviews	18
Electronic Records Management	19
Personal E-Mail	20
Legislative Review	21
Health Privacy Legislation	22
Educating our Children	22

ANNUAL REPORT 2008/2009

Nunavut Information and Privacy Commissioner

COMMISSIONER'S MESSAGE

In last year's Annual Report, I indicated that my office had had, by far, the busiest year since I assumed the office of Information and Privacy Commissioner. By contrast, 2008/2009 may have been the quietest year. I would like to think that this lack of business for my office is largely a result of the good work that is being done the ATIPP Coordinators in each of the public bodies, whose job it is to oversee these matters. Perhaps it has to do with the fact that the Government of Nunavut and its public bodies have established a strong corporate culture which embraces the ideals of the *Access to Information and Protection of Privacy Act*. To an extent, I think that both of these factors have played a role. From my perspective, the ATIPP Coordinators are working hard to make sure that Requests for Information are dealt with thoroughly and with the least number of exceptions being applied. I am also encouraged by what I see as the commitment of the Government of Nunavut to encourage openness in access to information matters. Nunavummiut deserve to have an access and privacy system that is easy to understand and robust in its implementation. They should be able to easily use the Act to obtain information, to challenge government actions and to keep public bodies accountable to the people.

The British Information Commissioner outlined his vision for his constituents in his 2008 Annual Report. He would like to see:

- A society where information rights and responsibilities are respected by all.
- Organizations that inspire trust by collecting and using personal information responsibly, securely and fairly;
- People who understand how their personal information is used, are

> Data protection is crucial to the upholding of fundamental democratic values: a surveillance society risks infringing this basic right.
>
> Thomas Hammarberg, the Council of Europe's Commissioner for Human Rights

aware of their rights and are confident in using them;

- Public authorities that are open and transparent, providing people with access to official information as a matter of course;
- People are aware of their rights of access to official information and are confident in using them.

This is a vision I believe that we should all strive for. Achieving that kind of robust system is possible, but requires more than a good oversight system. It requires ongoing review of the legislation to ensure that it meets the ever changing realities of the technological world. It requires well trained ATIPP Coordinators who can work together as a network to ensure appropriate and consistent application of the Act in all public bodies. Another absolute is a comprehensive training program for all new and existing public sector employees and contractors so that there is no confusion about what the rules are. It is, of course, helpful to have a comprehensive and practical manual that explains statutory requirements in plain language with checklists and precedents to assist when issues arise.

Perhaps most importantly of all, however, is a modern and effective information management system and strong policies about information management that are strongly enforced. Information is a necessary commodity in today's world. Misuse or mismanagement of that information, however, can be a toxic liability. A good information management system requires clear lines of accountability and responsibility, coherent policies and procedures, and rigorous enforcement of those policies. That kind of system is in place for paper records. That system does not work nearly as effectively, however, when dealing with electronic records, and most particularly, when trying to apply it to e-mail communications.

As technology advances at lightning speed, the modern workplace is becoming more and more digital and the rise of the electronic record is unprecedented. The use of word processing programs, spreadsheets, presentation programs, digital audio and video, electronic mail, and more has become so commonplace that it is now hard to imagine how people managed just a decade ago, let alone

> The government should not keep information confidential merely because public officials might be embarrassed by disclosure, because errors and failures might be revealed, or because of speculative or abstract fears,.
>
> President Barrack Obama, January 22nd, 2009 Memo to the Heads of Departments and Agencies

50 years ago.

As noted by the former Assistant Information and Privacy Commissioner for Newfoundland and Labrador, Sandy Hounsel, in a paper prepared for presentation to the 5th International Conference of Information Commissioners:

> A crucial aspect of the modern records management system is the explosion over the last number of years of electronic information. The modern workplace has become more and more digital and our reliance on electronic records and databases is unprecedented. It is estimated that more than 90% of all records being created today are electronic.
>
> There is no doubt that the advantages are numerous. We can search it, cut and paste it, update it in real time, e-mail it, automate it, audit it, secure it, and control it in ways that paper-based systems simply would not allow. Ultimately, this allows us to work faster, save money and accomplish much more with significantly less effort.
>
> However, organizations often have difficulty cataloguing, organizing and preserving this information, while maintaining a reasonable ability to access it. This is in part due to the failure of many organizations to properly recognize and manage the records management life cycle. This life cycle is equally relevant to both paper records and electronic records, a fact often overlooked by these organizations. More importantly, however, many organizations appear to be overwhelmed by the volume and variety of electronic records. The technology has simply surpassed the capacity to react appropriately.

.....

I am increasingly concerned about the management of electronic records. E-mail, in particular, does not appear to be well managed. As far as I am aware, every employee is left to manage their own e-mail system in their own way. There is no uniformity and no apparent policies beyond the very basic rules. What is saved and what is discarded seems to be in the hands of each individual employee. Many, if not all, employees use the

Citizens entrust their governments with power through elections, and with resources through the payment of taxes. Those who are entrusted with this power bear a responsibility not only to serve, but also to inform citizens and encourage the public to participate in their decisions and actions. - It is citizens, after all, who should ultimately be the source of power, as they bear the consequences of its abuse

Excerpt from the Web Site of Transparency International

government e-mail system for personal correspondence, without fully understanding that those records may well be the subject to an Access to Information request. Once that request is made, it would have to fall into one of only a very few, narrow exemptions in order to escape disclosure. No access to information system can work properly without good file management systems, and that includes electronic records. As noted by the Information Commissioner of the United Kingdom in a recent publication:

> Getting data protection and privacy right is central to people's lives and to the good reputations of organizations. Freedom of information has become a firmly established part of the fabric of public life. Both underpin modern democracy and public involvement in politics; both focus on the liberties of British life; and both are pivotal to the relationship between state and citizen.

Managing electronic records in a consistent and well established manner is just as important as managing paper records. This is not a problem unique to Nunavut. It is, in fact, one of the primary issues being faced by all governments, large and small, in Canada and abroad. Without good records management practices, access to information becomes impossible. Without the ability to access information from government, democracy is at risk. It is certainly a challenge, but one that must be met.

The stockpile of government information has been liquefied – broken down into a vast pool of elements whose significance, taken independently, is not easily grasped.

Excerpt from *Blacked Out: Government Secrecy in the Information Age* by Alasdair Roberts (New York: Cambridge University Press, 2006

THE ROLE AND MANDATE OF THE INFORMATION AND PRIVACY COMMISSIONER

Nunavut's *Access to Information and Protection of Privacy Act* (ATIPPA) came into effect prior to division on December 31st, 1996. When Nunavut was created, the Act became part of the law of Nunavut. It binds all Territorial Government departments and agencies and establishes the rules about how Territorial government agencies can collect, use and disclose personal information. It also outlines a process to allow the public to gain access to government records. The office of the Information and Privacy Commissioner (IPC) is created by the legislation to provide independent advice and review on questions that arise in the implementation of the Act. The IPC is an officer of the Legislature and is appointed by the Commissioner of Nunavut on the recommendation of the Legislative Assembly. She reports to the Legislative Assembly of Nunavut. As an independent officer, the IPC can be only be removed from office "for cause or incapacity" on the recommendation of the Legislature.

The term "access to information" refers to the right of the public to have access to general records relating to the activities of government, ranging from administration and operations to legislation and policy. It is an important aspect of open and accountable government. Under the *Access to Information and Protection of Privacy Act*, the public is given the right to request access to all "records" in the possession or control of a public body and provides a process for such requests. Although the Act does provide protection from disclosure for some types of records, the exceptions to disclosure are narrow and finite. Exceptions to the open disclosure rule function to protect individual privacy rights, allow elected representatives to research and develop policy and the government to run the "business" of government.

The Supreme Court of Canada has clearly stated that exemptions to disclosure provided for in access to information legislation should be narrowly interpreted so as to allow the

> There is no human institution but has its dangers. The greater the institution the greater the chances of abuse. Democracy is a great institution and, therefore, it is liable to be greatly abused. The remedy, therefore, is not avoidance of democracy, but reduction of possibility of abuse to a minimum.
>
> Mahatma Ghandi

greatest possible access to government records.

As implied by the name, the Access to Information and Protection of Privacy Act also has rules which are focused on protecting individual privacy with respect to personal information held by government agencies. It also provides a mechanism which allows individuals the right to see and make corrections to information about themselves in the possession of a government body.

ACCESS TO INFORMATION

The Access to Information provisions of the *Access to Information and Protection of Privacy Act* apply to all government departments and most agencies, boards and commissions established by the government.

One of the roles of the Information and Privacy Commissioner is to independently review the decisions and practices of government organizations concerning access requests and to provide recommendations to public bodies with respect to those issues. These recommendations are made to the head of the public body involved, who must then make a final decision as to how the government will deal with the with the matter. If, in the end, the person seeking the information is still not satisfied with the response received, there is recourse to the Nunavut Court of Justice for a final determination of the matter.

Requests for information must be made in writing and delivered to the public body from whom the information is sought. Although forms are available, requests for information do not need to be in any particular form. The only requirement is that the request be in writing. This would include a request made by e-mail but where a request is made by e-mail, it may not be considered complete until the public body receives confirmation of the request with the applicant's signature. Requests for information are subject to a $25.00 application

Accountability and transparency go to the core of representation, they shed light on power structures in democracy they can illuminate bias and self-interest, and most importantly, lack of them can destroy legitimacy.

A.N. Tiwari

Information Commissioner ,Central Information Commission, India

fee except in cases where the information requested is the applicant's own personal information. In such cases, there is no application fee, although there may be a fee for copying records in certain circumstances.

When a request for information is received, the public body has a duty to identify all of the records which are responsive to the request and to respond to the request within 30 days. Once all of the responsive documents are identified, they are reviewed to determine if there are any records or parts of records which should not be disclosed for some reason. The public body must endeavor to provide the applicant with as much of the requested information as possible, while at the same time respecting the limited exceptions to disclosure specified in the Act. There are both mandatory and discretionary exemptions from disclosure provided for in the Act. Where the exceptions are mandatory, public bodies are prohibited from disclosing the records within the category. In other instances, the Public Body is given the discretion to determine whether or not to disclose certain categories of information, keeping in mind the purposes of the Act and the weight of court authority which requires public bodies to err on the side of disclosure.

Every person has the right to ask for information about themselves. If an individual finds information on a government record which they feel is misleading or incorrect, a request in writing may be made to correct the error. Even if the public body does not agree to change the information, a notation must be made on the file that the individual has requested a correction.

Legislation is tested and improved as a result of usage, and without people using it, much of FOI is pointless. Whose role is it to educate the public? I would say it is the responsibility of every government agency and every public official who interacts with the public. FOI should be embedded into all of government's dealings with citizens.

Megan Carter,
Director, Information Consultants Pty Ltd

PROTECTION OF PRIVACY

Part II of the *Access to Information and Protection of Privacy Act* sets out the rules about how public bodies can collect personal information, how they can use it once it has been collected and how and when they can disclose it to others. The Act also requires public bodies to ensure that they maintain adequate security measures to ensure that the personal information which they collect cannot be accessed by unauthorized personnel. This Part of the Act also provides the mechanism for individuals to be able to ask the government to make corrections to their own personal information when they believe that an error has been made.

As of yet, the Information and Privacy Commissioner has no legislated role in the review of complaints made by members of the public who feel that their personal information has been improperly collected, used or disclosed by a public body. Notwithstanding this lack of legislated authority, the Information and Privacy Commissioner will accept privacy complaints and will attempt to address the concerns of individuals in this situation.

A driver's license is proof that someone is allowed to drive a car. It is not a universal identity card. Nor is it an appropriate identifier for use in analyzing shopping return habits.

David Loukedelis

Information and Privacy Commissioner of British Columbia

REQUESTS FOR REVIEW

Under section 28 of the *Access to Information and Protection of Privacy Act*, a person who has requested information from a public body, or a third party who may be affected by the disclosure of information by a public body, may apply to the Information and Privacy Commissioner for a review of the public body's response to an access request. This includes decisions about the disclosure of records, corrections to personal information, time extensions and fees. The purpose of this process is to ensure an impartial avenue for review and independent oversight of discretionary and other decisions made under the Act.

A Request for Review must be made in writing to the Information and Privacy Commissioner's Office within 30 days of receiving a decision from a public body under the Act. There is no fee for a Request for Review.

When the Information and Privacy Commissioner receives a Request for Review, she will take steps to determine what records are involved and obtain an explanation from the public body as to why they responded in the manner they did. In most cases, the Commissioner will receive a copy of the responsive documents from the public body involved and will review the records in dispute.

In some cases, it may be necessary for the Information and Privacy Commissioner to attend the government office to physically examine the public body's files.

Generally, an attempt will first be made by the Commissioner's Office to mediate a solution satisfactory to all of the parties. In several cases, this has been sufficient to resolve the issues between the Applicant and the public body. If, however, a mediated resolution does not appear to be possible, the matter moves into a more in depth review.

All of the parties involved, including the public body, are given the opportunity to make written submissions on the issues.

In the 2008/2009 fiscal year, the Information and Privacy Commissioner's Office opened only five (5) files in contrast to 35 opened in 2007/2008. Of these, one was a request by a public body for comment about the scope of the application of the Act. Three were Requests for Review with respect to Access to Information requests and one was a privacy complaint. The requests involved four departments:

- Department of Education
- Department of Human Resources
- Department of the Executive
- Arviat Health Centre

The Information and Privacy Commissioner issued four Review Recommendations in 2008/2009, down from 16 in 2007/2008.

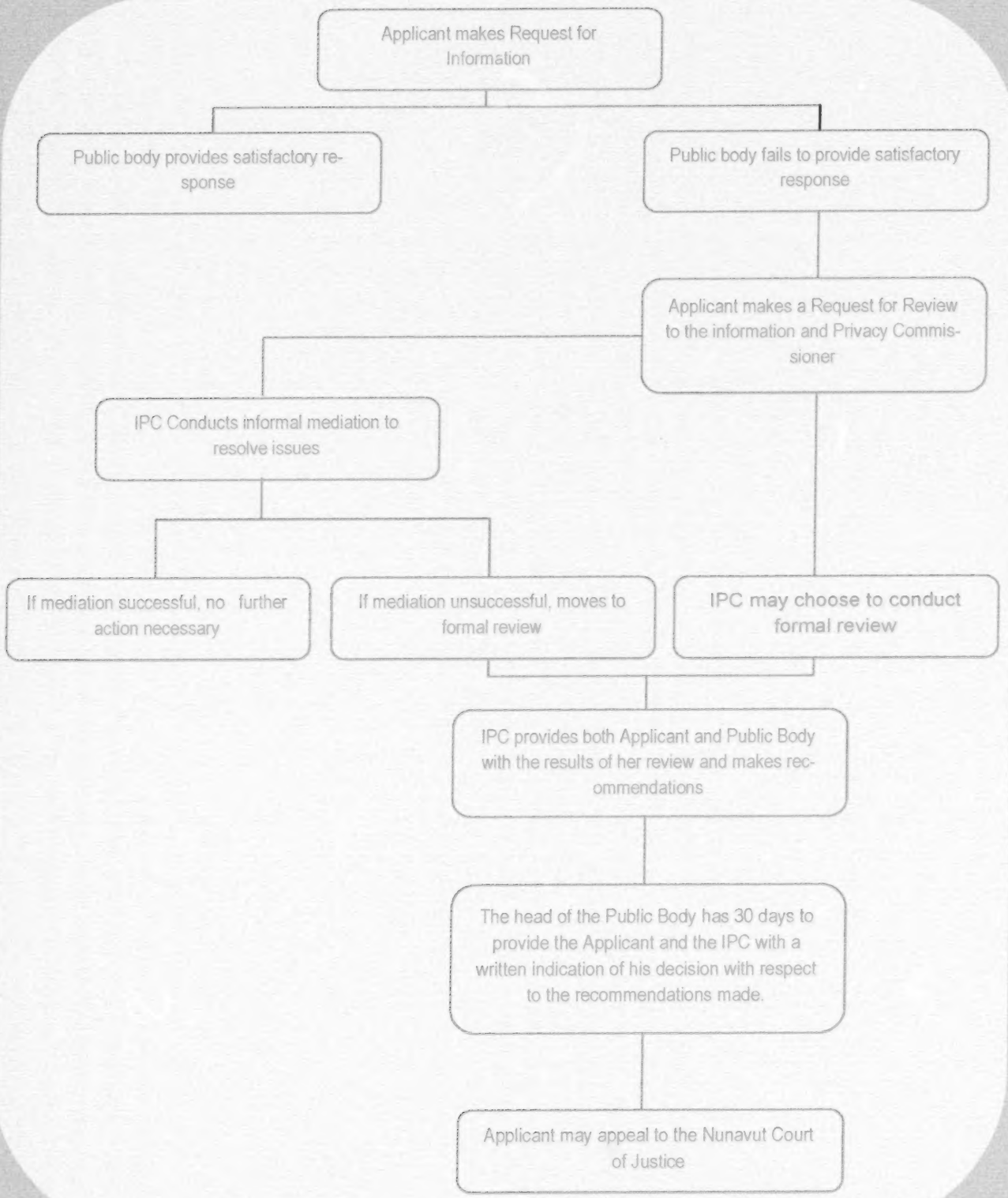
One Request for Review was considered abandoned when the IPC did not receive a response to her request for further details about the issues raised.

General surveillance raises serious democratic problems which are not answered by the repeated assertion that those who have nothing to hide have nothing to fear. This puts the onus in the wrong place: it should be for states to justify the interferences they seek to make on privacy rights.

Thomas Hammarberg,

The Council of Europe's Commissioner for Human Rights

MAKING AN ACCESS TO INFORMATION REQUEST


Applicant makes Request for Information
Public body provides satisfactory response
Public body fails to provide satisfactory response
Applicant makes a Request for Review to the information and Privacy Commissioner
IPC Conducts informal mediation to resolve issues
If mediation successful, no further action necessary
If mediation unsuccessful, moves to formal review
IPC may choose to conduct formal review
IPC provides both Applicant and Public Body with the results of her review and makes recommendations
The head of the Public Body has 30 days to provide the Applicant and the IPC with a written indication of his decision with respect to the recommendations made.
Applicant may appeal to the Nunavut Court of Justice

REVIEW RECOMMENDATIONS MADE

Review Recommendation 08-43

In this case, an Applicant sought information relating to a "Request for Proposals". The Applicant was seeking information about how each of the companies which had bid on the proposal had been rated under the Nunavummi Nangminiqaqtunik Ikajuuti Policy (NNI). The companies who had submitted proposals were asked whether or not they objected to the disclosure of this information. Two of the companies consented, one objected. Based on all of the circumstances, the public body decided to disclose the information requested, notwithstanding the objections from one of the companies. The company who had objected then asked my office to review that decision.

The public body identified only one record responsive to the request, which was a one-page record in the form of a chart showing the names of the companies who had submitted proposals and the total number of points awarded to each of the proponents under the NNI policy.

The third party company argued that the disclosure of the record would reveal how it conducted its business affairs and, in particular, would reveal the confidential relationships between the operation of the parent company and its subsidiaries. They felt that the disclosure would result in harm to their business.

The Information and Privacy Commissioner considered the position of the third party company. Noting that the onus was on the company in this case to establish that the information fell under one of the exceptions to disclosure, she indicated that she did not feel that the company had met that onus. She was not convinced that the disclosure of the rating points alone would reveal anything significant about the company or how it conducted its business affairs, pointing out that it might have been different if the record had included an indication of the reasons that the points were awarded.

The Information and Privacy Commissioner recommended that the record

> It is not sufficient simply to say that it is so. It is also necessary for the company to establish that the information is a secret and cannot be otherwise discovered with reasonable efforts. In the end, the Company has not provided me with enough to satisfy me that the information in question constitutes a trade secret, or that its disclosure might result in harm or improper benefit
>
> Elaine Keenan Bengts
> Review Recommendation 08-43

be disclosed.

The public body accepted the recommendation.

Review Recommendation 08-044

In this case, the Information and Privacy Commissioner considered two Requests for Review involving the same applicant together. The Applicant had requested the same information about himself from two different government departments. There were a very large number of records identified (more than 3500 pages between the two departments). Notwithstanding the volume of records provided to the Applicant, he felt that he had not received all of the records he had requested and asked the Information and Privacy Commissioner to review the response he had received.

The Applicant was specifically interested in knowing how much in the way of public funds had been expended on certain dealings involving him and his family. One of the things that the Applicant was interested in know was how much had been paid to lawyers in dealing with his issues. He wanted to know how much had been paid to the Legal Aid lawyer who represented him on the case, and how much had been spent on lawyers for the public bodies. The public bodies had disclosed the amount paid to private sector lawyers acting for the government but had not disclosed the amounts paid to the Legal Aid lawyer who had represented him. Nor had he been provided with a breakdown of amounts paid to in-house government lawyers in dealing with the issue.

He was also concerned that he had received very little information about the cost of services provided by non-legal private sector organizations in relation to his case.

The Information and Privacy Commissioner acknowledged that some of the information, particularly specific information about what had been spent on Legal Aid and in-house government lawyers was simply not available. She recommended that the public bodies follow up to determine whether they could obtain further information about the amounts paid to any private sector Legal Aid lawyer who had provided services to the Applicant. She also acknowl-

In this case, both the public bodies were very careful about allowing as much disclosure as possible and I applaud them for that approach

Elaine Keenan Bengts

Review Recommendation 08-044

edged, however, that lawyers working as "in-house" counsel for the Government of Nunavut, whether they worked for Legal Aid or in some other capacity, do not maintain time records indicating how much time they spend on any particular file or matter. As a result, the information that the Applicant was seeking was simply not available at least insofar as it related to the costs of in-house counsel.

She further recommended that the public body use their best efforts to determine the specific amounts paid to non-legal outside agencies for or on behalf of the Applicant and to provide him with that list within 60 days.

The recommendations made were accepted.

Review Recommendation 08-045

In this case, the Information and Privacy Commissioner received a complaint from an individual who felt that the Department of Education, and in particular the student loans program (FANS), had misused his personal information. He alleged that on two occasions when he had received forms to complete, the forms had been partially completed but with another person's personal information. He had taken the matter up with the FANS administrative staff, but was not satisfied that any appropriate steps had been taken to address his concerns. His concerns escalated when he was briefly put on "probationary status" by FANS, a status that was later revoked as being done in error, but with no further explanation being given.

When responding to the complaint, the public body acknowledged that their file in connection with the Complainant's FANS funding was incomplete and that they had had some records management problems which had affected a number of student records, including the Complainant's . The public body further advised that the Auditor General had raised concerns about the record keeping within the FANS program and had made a number of recommendations which were, at the time, in the process of being implemented.

In her review, the Information and Privacy Commissioner acknowledged that it appeared that the public body was addressing their records man-

Government agencies which hold significant amounts of personal information, such as health, education and housing, should have someone designated as the "chief information officer" whose responsibilities go beyond simply acting on access and privacy requests and include the management of records, record keeping and the security of records.

Elaine Keenan Bengts

Review Recommendations 08-045

agement problems. She found that there was no evidence that the Complainant's personal information had been improperly used or disclosed, but raised concerns about the public body's failure to keep records containing personal information in good order and secure from any possible misuse or improper disclosure. She recommended that employees working within the Government of Nunavut who are likely to be collecting or using the personal information of others be given specific training in access and privacy matters as a mandatory part of orientation and that refresher courses be required on an ongoing basis for those employees..

She also recommended that government agencies which hold significant amounts of personal information about the people of Nunavut, such as health, education and housing, should have an employee designated as the "chief information officer" whose responsibilities include the management of records, record keeping and security of records and that this person should have sufficient seniority and authority to act when issues arise, to create rules, policies and guidelines for the handling of records and to have responsibility generally over records management.

The Recommendations were accepted in part.

Review Recommendation 08-046

In this case the Applicant was not satisfied with the response that he had received to a request for information he had made regarding the calculation of bonuses paid to those in management positions a particular government department for a particular year. He had asked for information showing how the bonuses were calculated. The response received included two copies of a spread sheet with everything but the headings and the information which related to the Applicant blacked out. He received no correspondence or notes which might indicate what factors went into the calculation of the bonuses or even how his particular bonus had been set.

The Information and Privacy Commissioner noted that, by definition, a bonus is something granted for extra effort or a job well done and, even

The concern I have with the search is not the *bona fides* of it, but whether or not the scope of the search was wide enough to capture all responsive records.

Elaine Keenan Bengts

Review Recommendation 08-046

when a bonus is given as a result of a contractual provision, there is normally a discretion to be exercised, which would generally involve some discussion or an exchange of information between those responsible for making those decisions. In her opinion, it was not surprising, therefore, that the Applicant was skeptical about the thoroughness of the search for records when no documents were discovered that would suggest such discussions took place.

Although the Information and Privacy Commissioner was satisfied that there was a *bona fide* search for the records requested, she was not convinced that the search was as thorough as it should have been, particularly in terms of the search of electronic records. She pointed out that the effectiveness of a search for electronic records will be limited by the search parameters entered. The Information and Privacy Commissioner recommended that the search for records be redone with expanded search parameters.

The recommendation was accepted in part.

You can put an amazing security system in place, but if nobody understands how to use it, it will go wrong. It's all about the human factor...

Security training can't just be about ticking the box, it's got to be about making sure that people understand the everyday rules, and why they are there. ... It has to be part of people's everyday lives, so that they can relate to what you are asking them to do.

Martin Smith, Chairman and Founder, The Security Company

LOOKING AHEAD

Every year I make some recommendations for change with a view to making the process more accessible, effective and efficient. I have to confess to some frustration that there have been very few of those recommendations which have received any follow up by the Legislative Assembly. A number of the recommendations which follow have been made more than once. Some of them, which I consider particularly important, have been repeated in each of my Annual Reports dating back at least eight years. Although perfection is not possible, improvement is, and I encourage the Legislative Assembly to consider giving some priority to those recommendations which have been made over and over again.

1. Privacy Oversight

The *Access to Information and Protection of Privacy Act* outlines rules and regulations with respect how government can collect, use and disclose personal information. One of the goals of the Act is to ensure that the personal information that public bodies have about people is properly managed, that it is used only for the purposes it is collected and that it is not disclosed except in accordance with the Act. The rules are clear and focused. Unfortunately, however, they are unenforceable. There is no mechanism provided for in the Act to ensure compliance or allow redress when the rules are not followed. The only provision which deals with breaches of the privacy rules under the Act is Section 59 (1) which provides that any person who knowingly collects, uses or discloses personal information in contravention of the Act or the regulations is guilty of an offence punishable on summary conviction and liable to a fine not exceeding $5,000. This does not serve as a deterrent, nor encourage public bodies to give the privacy protections inherent in the Act the attention they deserve. This is so for a number of reasons.

> The second deadly sin is to pretend to Freedom of Information but to provide so many exceptions and derogations from the principle as to endanger the achievement of a real cultural change in public administration.
>
> Justice Michael Kirby, High Court of Australia (then President of the NSW Court of Appeal),

Firstly, section 59 will only apply where there is an intentional breach of the rules. In order to apply, the offender must have "knowingly" collected, used or disclosed personal information in contravention of the Act. Most of the privacy complaints that reach me are as a result of inadvertence or occur because not enough thought has been focused on the privacy aspects of the matter. In Nunavut, I have yet to receive a complaint that someone knowingly and intentionally collected, used or disclosed information contrary to the Act. Rather, the breaches complained of all resulted from inadvertence or lack of appropriate attention to privacy issues. This doesn't make the breach any more acceptable or any less harmful to the individual whose privacy has been breached, but the Act provides no redress and no solution.

Secondly, in order for Section 59 to apply, someone must take the step of having a charge laid under the Act and prosecuted by someone. That is unlikely to happen except in most egregious of circumstances.

Thirdly, fining someone for intentionally contravening the Act will not focus attention on problems in a way that will encourage review and changes so as to prevent the same kind of breach from happening again.

What is needed is a way to catch imperfections in the way in which government agencies collect, use and disclose personal information, and address those imperfections with new policies and procedures. It seems to me that a formal independent oversight function could address this issue and allow members of the public who feel that their personal information has been collected, used or disclosed contrary to the Act a way to address their concerns in a more effective way.

As Information and Privacy Commissioner, I have conducted informal reviews and made informal recommendations when I have received privacy complaints. There is, however, currently no obligation imposed on public bodies to co-operate with those investigations or to take any steps to address recommendations made. It seems to me that if the privacy rules were thought important enough to put into the legislation, they are important enough to deserve

Databases are not just lists, nor are they the digital equivalent of paper files. Structured databases enable the "querying" of data along novel lines, permitting machines to mine swaths of information, and from it to produce new information. The database state, therefore, is a machine bureaucracy that is actually run by machines. As such it promises to dehumanise both the public-service front line, and the people who rely on it most.

Becky Hogge

From: New Statesman, April 30, 2009

a way in which to monitor and assess whether they are being followed.

I therefore recommend that amendments be made to the Act to allow for a review process where there is a concern that someone's personal information has been improperly collected, used, or disclosed.

This has been a recurring recommendation and one that needs to be addressed to ensure that the people of Nunavut continue to have the same level of privacy protection as most other Canadians.

2. Time for Requesting Reviews

As currently worded, the *Access to Information and Protection of Privacy Act* allows an Applicant only thirty days after receiving a response to a Request for Information to ask the Information and Privacy Commissioner to review that decision. This is really a very short time frame when one takes into consideration the often slow delivery of conventional mail in the north and the fact that people do not always have fax machines or computers at their disposal to communicate more quickly. Over the years, there have been numerous instances in which a Request for Review has been received in my office a day or two after the end of the 30 day period.

Because the Act does not give the Information and Privacy Commissioner any jurisdiction to review a request made after the deadline, or to extend the time where appropriate, the Request for Review cannot proceed when this happens. In a number of instances, I have asked the public body to agree to disregard the fact that the Request for Review has been received after the limitation period so as to allow the review to proceed in any event. So far, public bodies have agreed to overlook the limitation period in these circumstances. There is, however, no obligation for them to do so and I can easily imagine a situation in which they might refuse. Should that happen, the alternative is for the Applicant to go back to the public body and make the same Request for Information a second time and start the process all over again. The only practical result is a duplication of effort for the public body and a delay for the Applicant. The process

The impact of poor records management goes far beyond the government's access and privacy regime. Within government, the lack of accurate and authoritative information results in poor decisions, failed programs and lost opportunities... The failure to maintain and protect records with high legal and intellectual property value results in increased liability and financial loss. The premature destruction of records with long-term archival value contributes to our collective historical amnesia and the loss of valuable knowledge.

Hon. John Reid
Information Commissioner of Canada

Annual Report
2002/2003

is already a fairly lengthy one and, to borrow a phrase, "access to information delayed is access to information denied".

The only instance that I can think of in which a limitation period for asking for a Request for Review has practical relevance is where the public body has decided to disclose information and a third party wishes to object to that disclosure. In such a case, unless the Request for Review by the third party is received within the 30 days, the information will be disclosed at the end of those 30 days and the third party who has missed the limitation period will be out of luck.

In order to correct this problem, it would be my recommendation that the Information and Privacy Commissioner be given discretion to extend the time for requesting a review in appropriate circumstances, except in the case where the issue involves a third party objection to the disclosure of information.

3. Electronic Records Management

This is a significant issue throughout the country. The push for the paperless society hasn't necessarily reduced the amount of paper that business and government uses, but the convenience and flexibility of digital medium has increased the volume of information that needs managing and has changed the dynamic of information and document management systems. The records management systems that worked in the papered world are simply unsuitable for the realities of the digital world. It is important, therefore, to find a consistent, clear and universal system to deal with the filing, storage, and security of electronic records. Unless electronic records can be properly categorized, catalogued, organized and preserved, the information in them will become inaccessible. If you don't know what you have, or where you can find it, it is tantamount to having lost it. Access legislation is based on a presumption that records are organized and accessible in accordance with some reasonable system so that they can easily be found, recovered and produced when needed.

This is a huge task which, as noted, is certainly not unique to Nunavut.

> Although we have seen massive change in the capability of organizations to exploit modern technology that uses our information to deliver services, that has not been accompanied by a similar drive to develop new effective technical and procedural privacy safeguards,
>
> Richard Thomas
> UK Information Commissioner

Some of the issues are as mundane as how to ensure continuing access to records stored with older technology when that technology changes. Most of us will remember computer punch cards, now gone the way of the dinosaur. That technology is only about 30 years old, but the information stored in that form is now all but inaccessible. Then came the 51/4 inch floppy disc, followed by the 31/2 inch ones. You'd be hard pressed to find a working computer today that had the necessary drives to read either of these mediums. Even if you can find a computer with the necessary hardware, is the software still available to allow access to those records?

Many of the reviews which I have conducted in the last number of years involve primarily e-mail records. There is always a concern with e-mail that the records have been properly preserved and filed and can be identified as responsive when an application for information is received. There seems to be no real government wide system for filing and storing e-mail communications. Each individual employee has their own system. One person might delete everything within a week, the next never delete anything. One person might have a very well organized electronic file system set up for everything they receive and the next leaves everything, uncategorized, in their general inbox. And where are the controls over what can be deleted from a desk top and what remains as a government record? There needs to be an effort to devise a system which is to be used by all government employees with consequences for improper storage. Without such a system, strongly enforced, the government will soon lose the ability to track and account for records created . When records cannot be found, the ability to hold government accountable is weakened.

4. Personal E-Mail

In the last few months I have been asked to deal with a request for certain e-mail records which were sent from a government computer, during regular working hours, under a government signature addressed to another government employee. The writer considered the content to be

I for one do not believe that a poor records management protocol is an appropriate enough reason to deny an applicant access to information that he or she is rightfully entitled to. This highlights the importance of handling all records, both electronic and paper, in a manner that is conducive to appropriate access, security and conservation.

Sandy Hounsel

Assistant Information and Privacy Commissioner for Newfoundland and Labrador

personal information. I disagreed and recommended the disclosure of the record. I have, in several previous Annual Reports, cautioned that there should be some very clear and well publicized rules regarding the use of government computers for personal e-mail correspondence. I understand that the Collective Bargaining Agreement allows for government employees to send and receive e-mail on their government computers under their government assigned e-mail address for matters not related to their work. This being the case, employees may think that the personal e-mails they send and receive via their government e-mail account are private. They are not. They are "records" within the definition of the Act and are, therefore, subject to an Access to Information request and to disclosure. I would, therefore, recommend that employees be reminded on an ongoing basis that, notwithstanding the fact that the Collective Bargaining Agreement allows personal use of government e-mail systems by employees, those communications are subject to the *Access to Information and Protection of Privacy Act* and may be the subject of an access request. They should be reminded often that caution should, therefore, be exercised when taking advantage of their government e-mail for personal communications.

5. Legislative Review

The *Access to Information and Protection of Privacy Act* is now 10 years old. There have been no substantive changes to the legislation and no real review of the legislation or its effectiveness. Sometimes the impetus for change will come from change itself. With elections behind us and a new Legislative Assembly on board with many new members, perhaps this is the time to consider giving some priority to a review of the *Access to Information and Protection of Privacy Act* to ensure that it continues to meet the goals of open and accountable government and the protection of privacy. The world has changed dramatically in ten years, particularly in

A learning process needs to be introduced rapidly, aimed at the youngest users who are at least aware of the risks inherent in their assiduous use of new communication technologies. If nothing is done today, could future generations claim tomorrow that their privacy is "safe"?

Excerpt from the Web Site "Protecting Privacy in a Borderless World", 30th Annual Data Protection Commissioner's Conference, Strasbourg, France, October 2008

its capacity to move and exchange information, and if the legislation is to continue to be effective, it must change with and address those technologies.

5. Health Privacy Legislation

The country is charging head long into the era of electronic health records and electronic medical records. Every jurisdiction in Canada, other than Nunavut, has now either passed health specific privacy legislation or is developing such legislation to address the very real privacy concerns raised by electronic records. The issues are significant and complicated. More to the point, the move to electronic medical records seems inevitable. A national system of managing those records is being developed as we speak . All Canadian jurisdictions have been meeting for the last several years to talk about how such an integrated electronic medical records system would work and what such a system would need to ensure security and privacy of medical records. It would no doubt be a positive development for every person in Canada to be able to access their electronic medical records, no matter where they happen to be in the country at a given moment. The challenges of such a system, however, are enormous. The work being done to create such a system is very real and if Nunavut does not begin to consider these issues and determine its own rules for the protection of health records, it will find itself with few choices and the solutions already dictated by those jurisdictions which have led the charge, with little consideration for the unique needs and realities of health care in the north. I would strongly recommend that steps be taken to begin the process of developing health sector privacy legislation as soon as possible.

We still have public trust.. But, trust is not a renewable resource -- once it is lost it may not be regained.

Mary Lysyk,
Policy Adviser for
Health Canada

7. Educating our Children

Continuing on a theme I began last year in my Annual Report, I would like to see more attention given to developing school curriculums which will include guidance and direction to our children in their use of the internet applications. Social networking sites

have increasingly become the communication vehicle of choice, particularly among young people. Most young people, however, fail to understand the inherent risks of sharing too much information with the people within their networks. Nor do they appreciate the fact that, unless they take steps to protect their information, it is not only their friends, but millions of other people as well who can read their posts and see their pictures. In the words of Ann Cavoukian, Information and Privacy Commissioner for Ontario:

> Online social networking has progressed well beyond the point of being a passing fad – it has become the preferred way that millions of people choose to communicate, socialize and interact, on a daily basis. As with most innovations that have a major impact on the lives of a vast number of people, there can be serious, unexpected results if users, particularly the young, are not made aware of the potential implications. There is widespread concern that young people do not understand the privacy risks associated with revealing too much information about themselves online, ranging from cyberbullying, identity theft and Internet luring, to jeopardizing future job prospects.

Times are changing and school curriculums should be changing as well. If children are going to be using these technologies, it is incumbent on the educational system to make sure they understand them and to give them the tools they need to use them safely. I recommend that steps be taken to include comprehensive instruction on new technologies, including instruction with respect to safety on the internet.

In terms of public awareness, all of the Canadian commissioners are currently working on a public awareness campaign aimed at young audiences, to help them understand the inherent risks to privacy and personal information that arise from using social networking sites.

Jennifer Stoddart

Privacy Commissioner of Canada in an address to the 30th Annual Data Protection Commissioners Conference , Strasbourg, France, October, 2008